Privacy Policy
For the
Communication Assets Survey and Mapping (CASM) Resource Finder (CRF)
Mobile Application

Overview

The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) developed and deployed the Communication Assets Survey and Mapping (CASM) Resource Finder (CRF) mobile application to provide authorized users with the capability to quickly and easily find the latest information for communications gateways, radio caches, and mobile communications units for the purpose of public safety interoperability using a smartphone or network connected tablet.

This policy informs users of the Department's policies regarding the collection, use, and disclosure of personal information when using the CRF mobile application.

Information Collected

In order to gain access to the CRF mobile application, a user must enter his or her CASM credentials at the log-in screen. The user's credentials will be transmitted to, and compared with the CASM user database which will provide the application with a response as to whether or not the user is authorized to access the application. Once authenticated, the application will access a user's geographic location only while the application is running in order to provide communications interoperability services. User information, including location information, is not stored by the application and is not transmitted to any system outside of the application.

Uses of Information

DHS does not use personal information from CRF users for any purpose beyond authentication and offering communications interoperability services. Personal information is only used to improve communications interoperability and will not be shared outside of the CRF application. Personal information, including location information, is not stored by the CRF application.

Information Sharing

DHS does not share personal information, including location information outside of the CRF application.

Application Security

The CRF mobile application operates locally on a user's mobile device and the user's session can be accessed only via that user's device; therefore, CRF user information is not transmitted over the internet. Personal information, including location information, is not stored by the CRF application. DHS recommends that users properly secure access to mobile devices using means supplied by the device manufacturer and operating system.

How to Access or Correct your Information

The CRF application leverages CASM user access credentials to authenticate users. Users may submit questions or concerns to CISA's Public Safety Tools team via the *Help* section in the CRF mobile application.

Analytics Tools

The CRF mobile application does not employ the use of any analytic tools.

<u>Privacy Policy Contact Information</u>

If you have questions about this Privacy Policy, you may contact the CISA Office of Privacy using the below contact information:

Email: NPPDPrivacy@hq.dhs.gov
Phone: (703) 235-1919
Mail: CISA Office of Privacy
      DHS Mail Stop 0380
      245 Murray Lane
      Arlington, VA 20598